
Segunda onda em VoIP: segurança
RNP
29 de maio de 2009

Roteiro

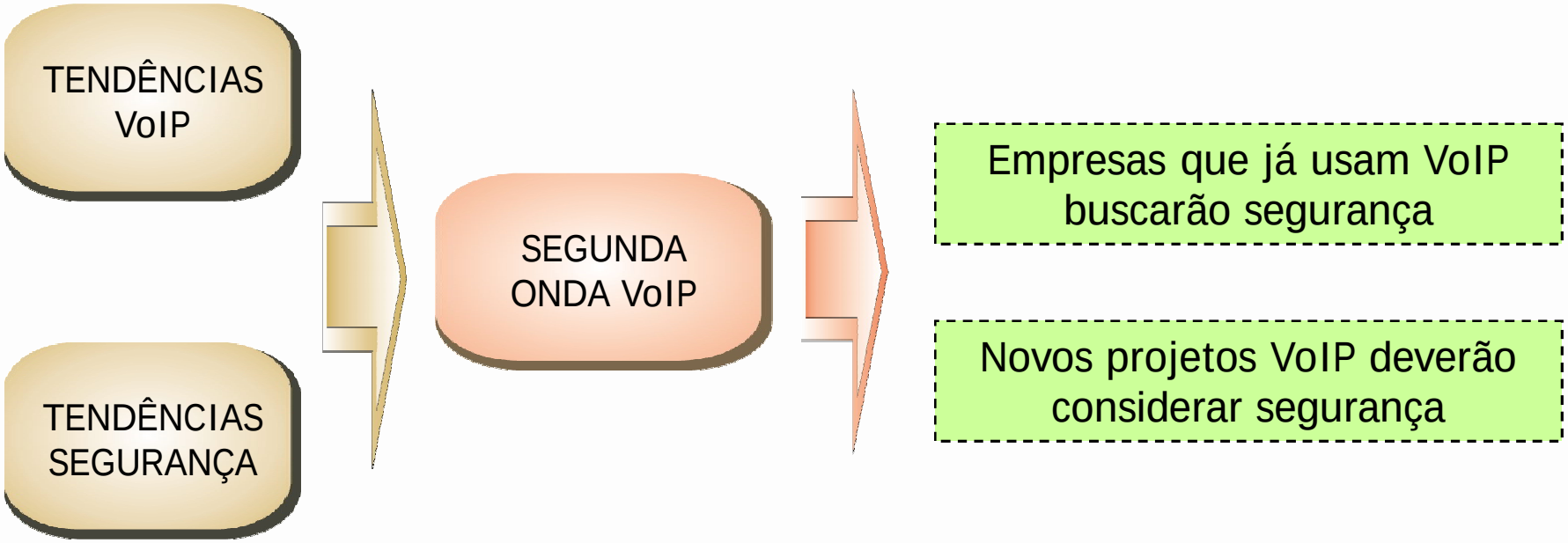
1. Motivadores VoIP
2. Segunda onda VoIP: segurança
3. Principais Ameaças
4. Últimos Ataques
5. Tipos / Apresentação de Ataques
6. Projeto VoIP Seguro CPqD
7. Conclusão

Motivadores VoIP

- Reduzir gastos de chamadas telefônicas
- Reduzir gastos com infra-estrutura
- Reduzir gastos com suporte e manutenção
- Convergência de redes
- Novas funcionalidades
- Novas instalações

OBS.: Segurança não é um fator motivador para VoIP

Segunda onda VoIP: segurança



Segurança em Telefonia (convencional)

- Phone Phreaking (tradicional)
  - Cup's Crunch (década de 60)

Blue Boxes (década de 70)

Segurança em VoIP

- Phone Phreaking (moderno)
  - Hacking da rede de telefonia via Internet
  - Fácil de obter “skills”
  - Conjunto de ferramentas emergentes distribuídas gratuitamente
  - Simples acessar a PSTN via gateways VoIP

As causas dos problemas de segurança em VoIP

- Implementações básicas
- Equipamentos mal gerenciados
- Arquitetura de rede VoIP mal projetada
- Falha em procedimentos operacionais
- Inexistência de uma política de segurança
- Falta de suporte técnico adequado
- Excesso de confiança nos fabricantes

Principais Ameaças

→ **Voz é um serviço crítico rodando sobre rede IP**

- Ambiente vulnerável a vírus, worms e DoS
- Roubo de identidade (número do telefone)
- Escuta clandestina (grampo telefônico)
- Redirecionamento de chamadas
- Sequestro de sessão
- Injeção de tráfego
- Toll Fraud

Últimos Ataques

The New York Times

Gadgetwise

Getting Smart About Personal Technology

May 18, 2009, 7:43 PM

Caller ID Fraud Is a Grim Reminder

By ROY FURCHGOTT

Security & Privacy

The Queens district attorney, Richard Brown, has taken down an identity theft ring that prominently used phone technology in its deceit, which serves as a reminder: Don't give out any personal information on the phone.

The moral to the story is this: If banks can be taken in by a spoofed call, so can you. Don't accept a caller ID number as proof of someone's identity.

Últimos Ataques

cnet news

May 19, 2009 4:00 AM PDT

Protecting yourself from vishing attacks

by Marguerite Reardon Font size Print E-mail Share 17 comments

You might have heard about online "phishing" scams designed to steal money from unsuspecting Web users, but now criminals are using another type of scam called "vishing" to commit the same crimes.

These companies likely used spoofed caller ID numbers to hide their identities from consumers and law enforcement authorities.

iWeb

THE TECHNOLOGY NEWS SITE

Organised criminals latch onto VOIP

BY ALEX KAYLE , JOURNALIST

READ IN THIS STORY:

- Flaws in VOIP

[Johannesburg, 19 May 2009] - Wiretap-friendly voice over Internet Protocol (VOIP) is not impervious to hacking, and unsecure VOIP is bad for society and good for organised crime.

Últimos Ataques

PBX hacking continues to threaten business owners

13.05.2009

PBX fraud, which is estimated to cost businesses in this country around €75m a year, is on the rise, and businesses are being encouraged to be vigilant and report suspicious activity to the authorities.

The Commission for Communication Regulation (ComReg) said last night that a recent PBX hacking incident, which has hit an Irish business in the wallet, has encouraged it to re-issue warnings to business about the ease with which PBX telephone fraud can occur.

"These incidents tend to occur at weekend periods when business premises are unattended," ComReg said.

Últimos Ataques

The Register®
Biting the hand that feeds IT

US military shows off hack-by-numbers battlefield gadget

Cyber warfare made easier

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 22nd May 2009 18:53 GMT

Free whitepaper – Opening new doors with HD Video and Telepresence

As the US military strives to boost its ability to wage cyber warfare, it's looking for ways to make it easier for non-expert soldiers on the front lines to wreak havoc on enemy networks.

Enter a new generation of attack devices that is packaged to be brought into the battlefield and used by non-specialists to penetrate satellites, voice over internet networks, and supervisory control and data acquisition systems. *Aviation Week* recently got a peek at one device and provided a rich description of its features.

Riser authors caller ID scam bill

GREG HILBURN • GHILBURN@THENEWSSTAR.COM • MAY 7, 2009

Read Comments(3) Recommend(2) Print this page E-mail this article Share

BATON ROUGE — Consumers who use caller ID to screen calls may find themselves victims of malicious pranks or fraud as part of a scam called caller ID spoofing, state Sen. Neil Riser said.

So Riser, R-Columbia, authored a bill that would make it a crime for callers who hide their true identities.

Tipos de Ataques

- **Eavesdropping**
  - RTP Playback
- **Hijacking**
  - ARP Spoofing
  - ENUM hijacking
- **Authentication**
  - Digest replay
  - Caller ID spoofing

Tipos de Ataques

- **Media Attacks**
  - RTP Injection
- **Social Attacks**
  - SPIT
  - Vishing
- **Firewall traversal**
  - Command shell channeling
- **Dial plan escalation**
  - CoS/CoR manipulation

Tipos de Ataques

- **Appliance hacking**
  - Equipamentos gerenciados inadequadamente

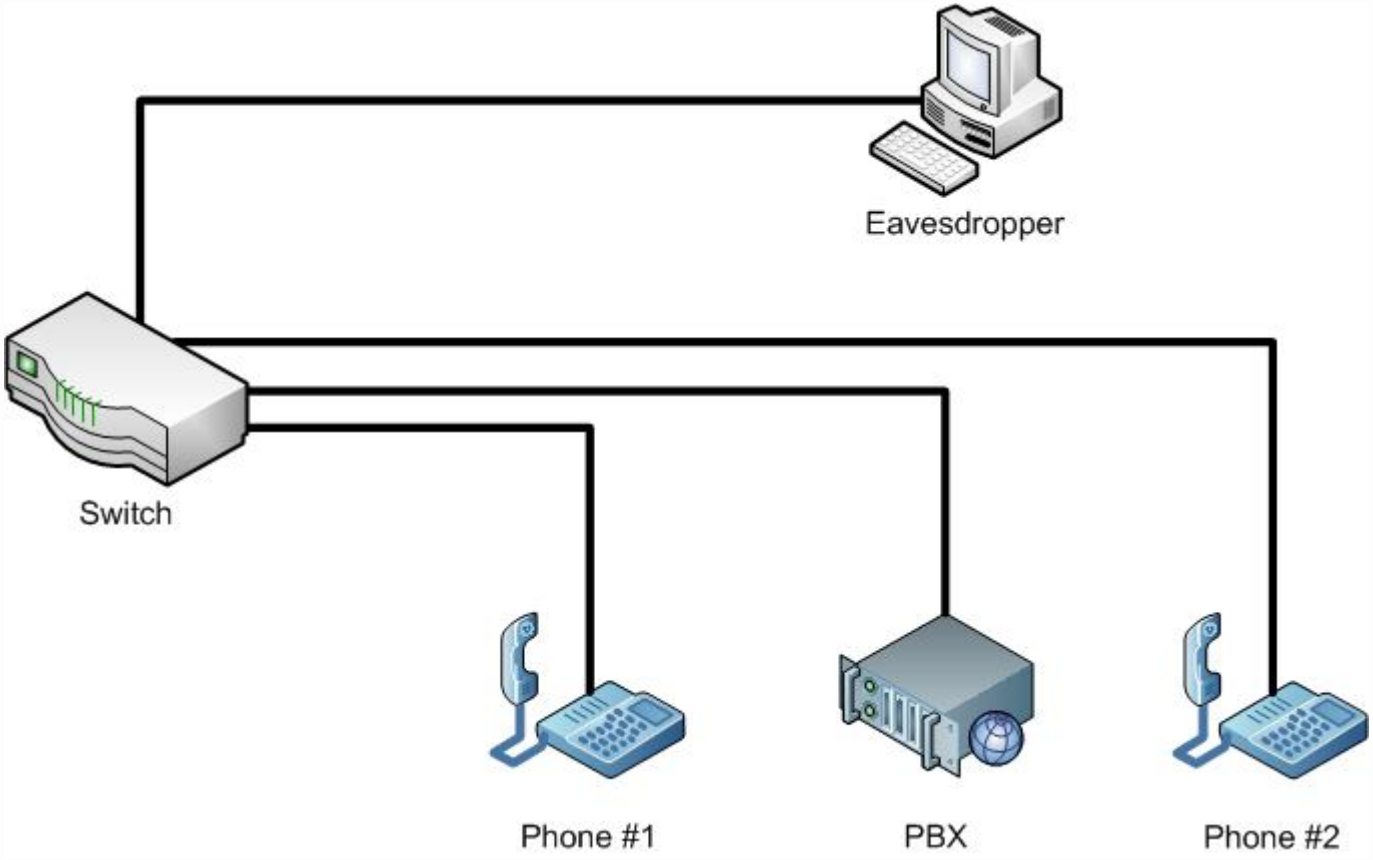
- **Toll fraud**
  - Gateways expostos
  - Manipulação de CDRs (Billing wipe)
  - Voicemail hacking (admin rights)

- **DoS**
  - Ataques a infra-estrutura

Apresentação de Ataque (1)

- Cenário 1
- **Eavesdropping: RTP Playback**
  - Como RTP Playback funciona

Cenário 1

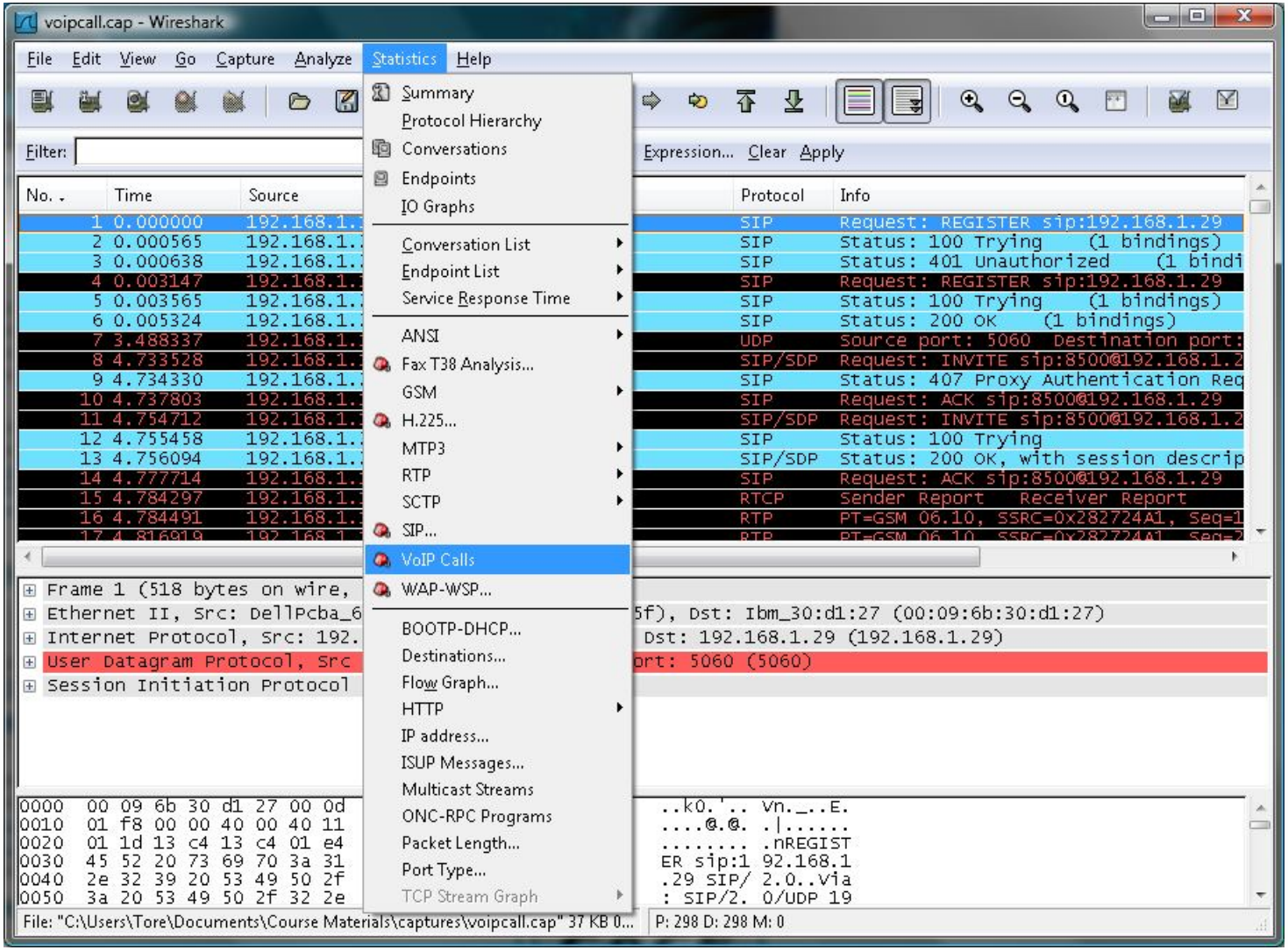


Eavesdropping: RTP Playback

- **Áudio pode ser reproduzido a partir de uma captura de pacotes não criptografados de chamada VoIP utilizando ferramentas livre, simples.**
- Requisitos:
  - Atacante deve ser capaz de interceptar o tráfego da chamada sem criptografia
- Procedimentos:
  - Capture uma chamada entre duas partes
  - Reproduza o audio utilizando o *Wireshark* (antigo *Ethereal*)

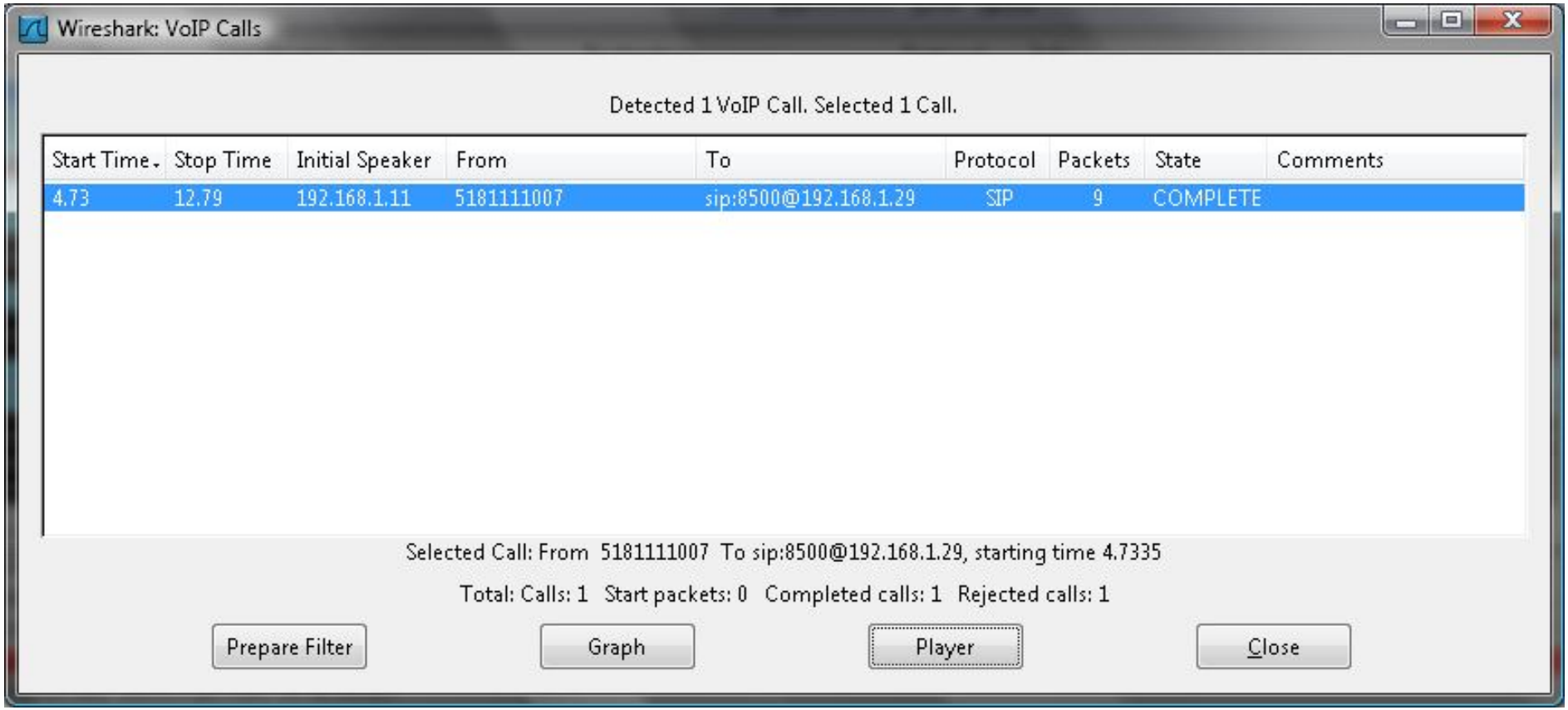
RTP Playback com o Wireshark

- Depois de realizar a captura, clique no seguinte item do menu:



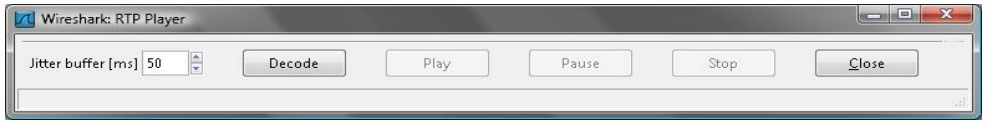
RTP Playback com Wireshark

- Selecione a mensagem que você deseja escutar e pressione ‘Player’:

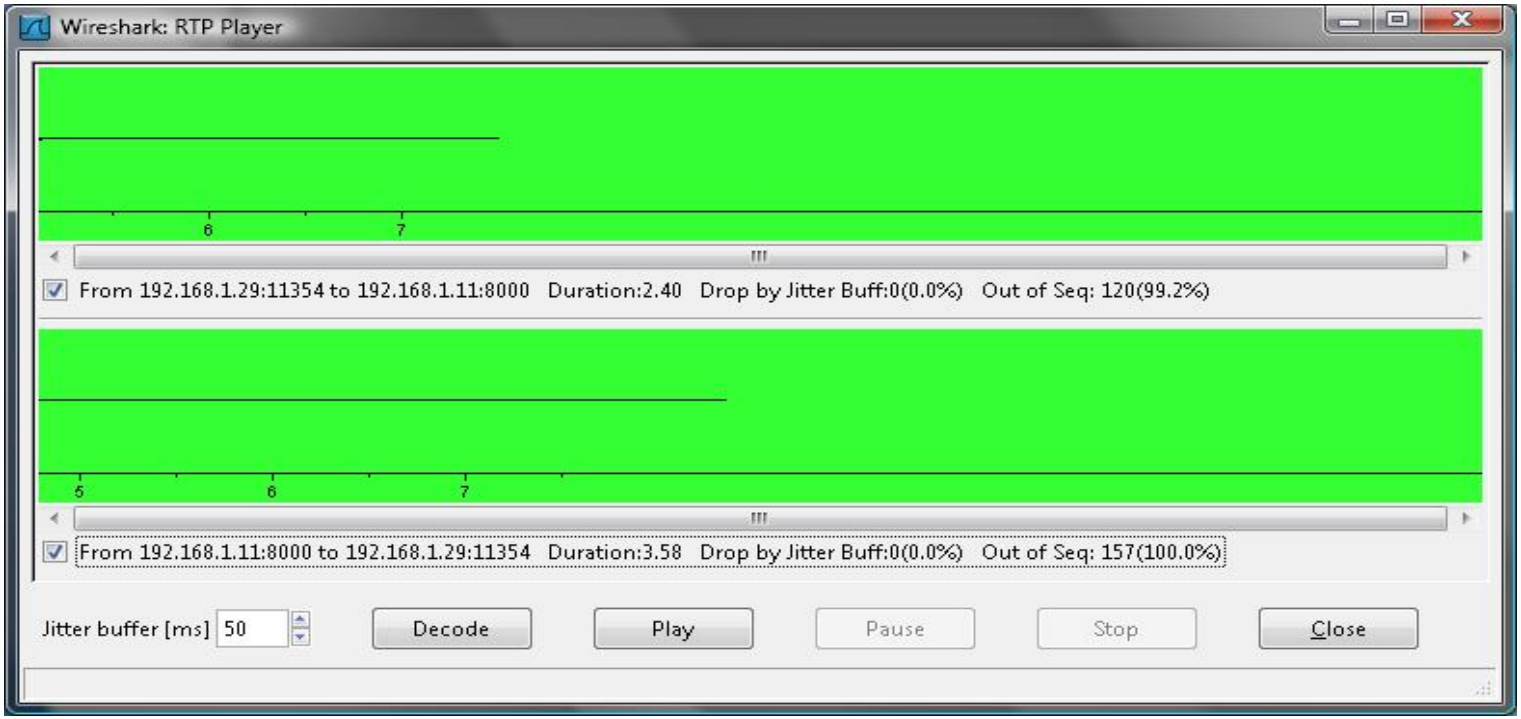


RTP Playback com Wireshark

Decodifique os fluxos.



Selecione um ou ambos os fluxos e pressione ‘Play’.



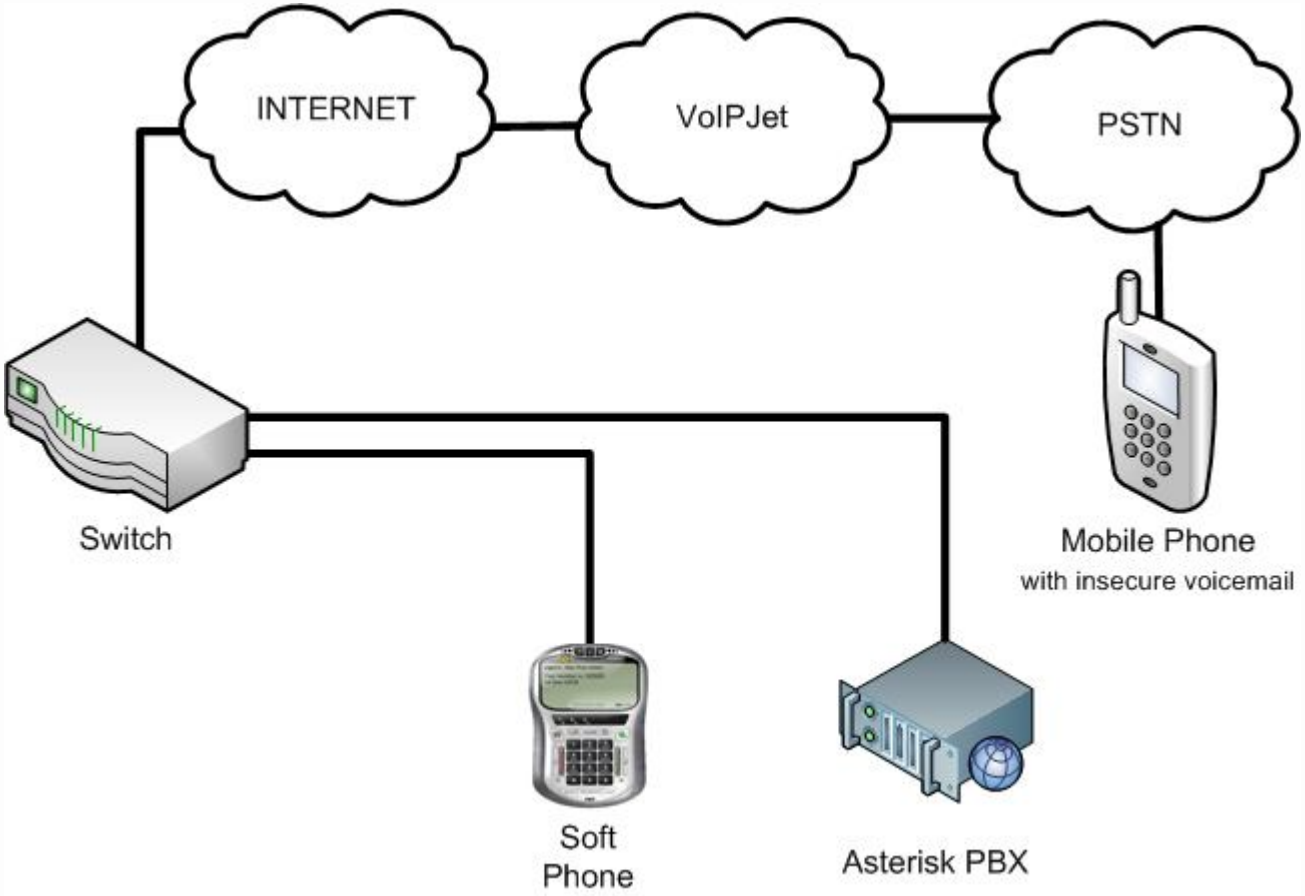
Prevenindo o Eavesdropping

- Utilize TLS/SRTP (or ZRTP) para criptografar a mídia VoIP
- Utilize IPSEC VPN's para criptografar troncos VoIP
- Utilize hardware de criptografia para proteger o envio de audio sobre um canal não seguro.

Apresentação Ataque (2)

- Cenário 2
- **Authentication: Caller-ID Spoofing**
  - Usando VoIP para realizar o acesso ao *voicemail* do telefone celular

Cenário 2


INTERNET
VoIPJet
PSTN
Switch
Mobile Phone
with insecure voicemail
Soft
Phone
Asterisk PBX

Authentication: Caller-ID Spoofing

- **Altere o seu outbound caller ID para explorar sistemas que utilizem caller ID para autenticação**
- Requisitos:
  - Soft phone, Asterisk box, & conta em provedor VoIP
- Procedimento:
  - Utilize um asterisk box para ajustar o seu caller id para o número de telefone desejado e realize a chamada
- Ação preventiva:
  - Não confie em caller ID

Alterando o Caller ID no Asterisk

- Entrada no Asterisk PBX: sip.conf

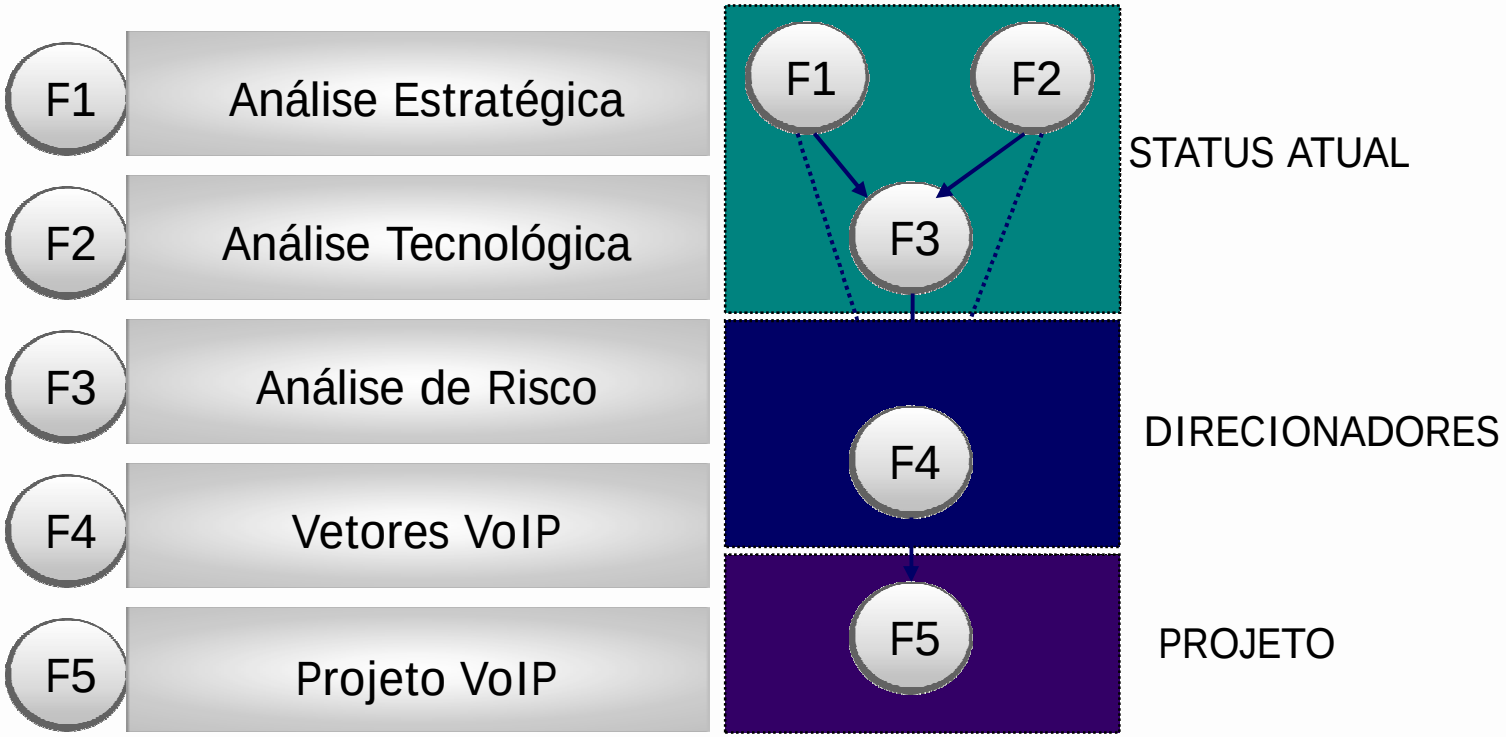
```
[16179591002]
type=friend
regexten=16179591002
secret=password
host=dynamic
nat=yes
canreinvite=no
disallow=all
allow=ulaw
mailbox=16179591002@default
context=longdistance
callerid=16179591002
```

Simplesmente altere o valor para 1617959XXXX e reload.

Prevenindo o Caller-ID Spoofing

- **É possível impedir o Caller ID spoofing?**
- As regras:
  - Você não deve confiar em Caller ID
  - Nunca utilize Caller ID para autenticação
  - Melhores práticas:
    - Sempre identifique a origem
    - Autenticação pode substituir a identificação da origem
    - Identificação da origem não é substituto da autenticação

Projeto VoIP Seguro: Abordagem



Projeto VoIP Seguro: Resultado

- Priorização da segurança, sem negligenciar a qualidade de serviço nem a funcionalidade
- Confiança no funcionamento é justificada pela análise e pela mitigação dos riscos de maior preocupação para a organização

Conclusão

- A tecnologia VoIP está se tornando vítima do seu próprio sucesso.
- VoIP geralmente proporciona economia, mas também oferece novos riscos.
- Implementar segurança sem comprometer o QoS é crítico

  Delay < 150 ms

  Jitter < 40 ms

  Packet loss < 3%

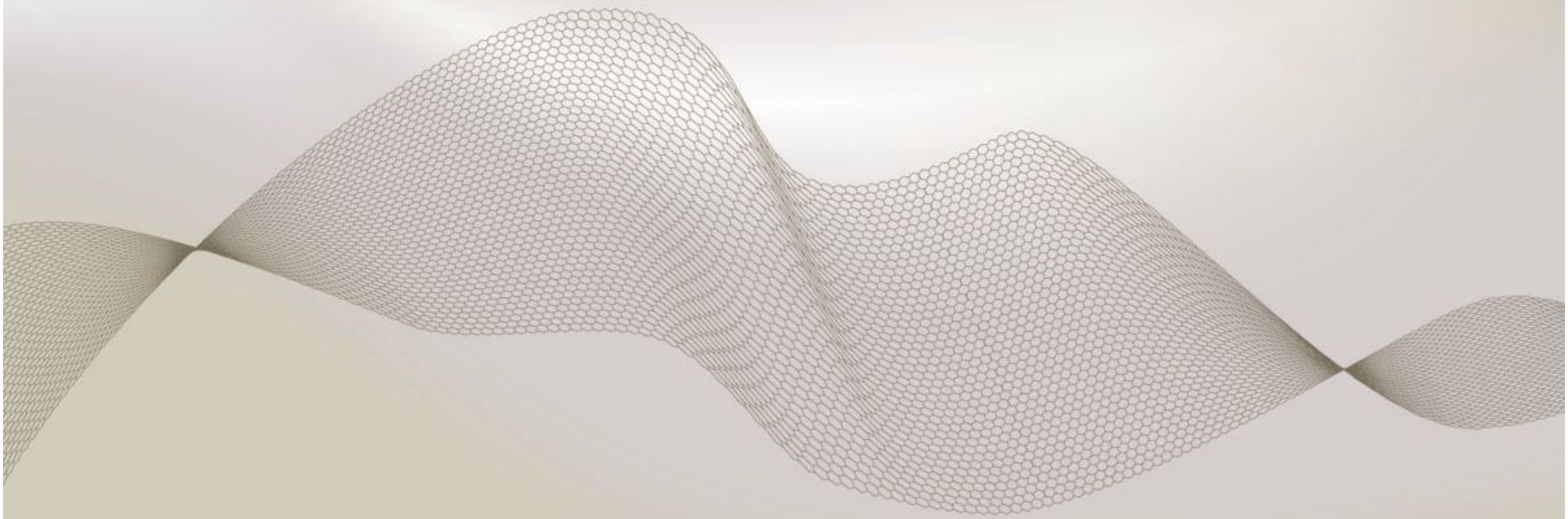
Centro de Pesquisa e Desenvolvimento em Telecomunicações

- O CPqD continua na vanguarda de Segurança em VoIP no Brasil e está posicionado para trabalhar com qualquer assunto relacionado a “VoIP Security”

PERGUNTAS ?

Alessandro Paganuchi
VoIP Security Professional, PCI DSS QSA
paganuch@cpqd.com.br
(19) 3705-5853

Obrigado !



www.cpqd.com.br

Referências

- http://gadgetwise.blogs.nytimes.com/2009/05/18/caller-id-scam-is-a-grim-reminder/
- http://www.siliconrepublic.com/news/article/12938/comms/firms-face-pbx-hacking-threat
- http://www.itweb.co.za/sections/internet/2009/0905191050.asp?O=FPTOP&S=Security%20Summit%202009&A=SSC
- http://news.cnet.com/8301-1035_3-10244200-94.html
- http://www.thenewsstar.com/article/20090507/NEWS01/90507001
- http://www.theregister.co.uk/2009